EXHIBIT A

ALTO LITIGATION

4 Embarcadero Center, Suite 1400
San Francisco, CA 94111

415.779.2586 General
415.306.8744 Fax

josh@altolit.com
www.altolit.com

December 21, 2020

Via Email

Felix Lee
flee@fenwick.com
Jennifer Bretan
jbretan@fenwick.com

Counsel for Temujin Labs

Re: DOCUMENT PRESERVATION NOTICE
***Temujin Labs Inc. v. Abittan, et al.*, No. 20CV372622 (Santa Clara County)**

Dear Counsel:

PLEASE TAKE NOTICE that all litigants are required to preserve documents, data, tangible things and electronically stored information potentially relevant to the issues in this case. Accordingly, you are required to preserve documents, data, tangible things and electronically stored information potentially relevant to the parties' claims or defenses in the above-captioned action, as well as the parties' claims or defenses in the draft complaint that was provided to you on December 20, 2020.

This letter serves as a discovery hold notice and advises you concerning your duty to preserve all manner of evidence. The duty to preserve is referenced as a "demand" from Ariel Abittan's counsel. This demand is broad and is a duty that arises under the law even though such materials may never be produced or demanded by counsel during litigation.

As used in this document, "you" and "your" means Temujin Labs Inc. (also known as "Findora"), Lily Chao (a/k/a Tiffany Chen, a/k/a Yuting Chen), Damien Ding (a/k/a Damien Leung, a/k/a Tao Ding) as well as any of their present or former employees, representatives, and/or agents, and any person or entity that has acted or is acting on behalf of and/or that controls or is controlled by any of the foregoing, including but not limited to Guanghua Liang, Selena Chen, Yang Ying, Jianrong Wang, and Xilei Wang.

The definition of "documents," "data," and "tangible things" may include: writings; records; files; correspondence; reports; memoranda; calendars; diaries; minutes; electronic messages; voicemail; e-mail; telephone message records or logs; text messages; computer and network activity logs; hard drives; backup data; removable computer storage media

such as tapes, disks, and cards; printouts; document image files; Web pages, cache and temporary Internet files; databases; spreadsheets; software; books; ledgers; journals; orders; invoices; bills; vouchers; checks; statements; worksheets; summaries; compilations; computations; charts; diagrams; graphic presentations; drawings; films; charts; digital or chemical process photographs; video; phonographic tape; or digital recordings or transcripts thereof; drafts; jottings; and notes. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata, is also included in this definition. Accordingly, you are required to preserve documents, data, tangible things and electronically stored information potentially relevant to the claims or defenses in this action, including but not limited to:

- All communications with and between you and present and former employees, representatives, agents, persons. or entities that have acted or are acting on behalf of, and/or that control Temujin Labs Inc., Eian Labs Inc. (f/k/a Porepsus Labs Inc.) ("Eian"), and/or Findora;
- All documents and communications related to Ariel Abittan, Eian, Benjamin Fisch, Charles Lu, Lakeside Garden Heritage LLC, Fourhair LLC, Guanghua Liang, Dan Boneh, Balaji Srinivasan, Rosario Gennaro, the Findora Ledger, Yang Ying, Xilei Wang, Selena Chen, John Powers, Benedikt Bunz, Juniper Ventures Partners LLC ("JVP"), Juniper Ventures Inc. ("JVI"), Ma Huateng, Tencent, Perfect World, China Orient, Tron, Jack Ma, Cathy Zhang, and the Zei cryptography library;
- All Telegram, Twitter, and other social media accounts owned or administered by you;
- All documents related to Temujin Labs Inc. and Findora's efforts to develop, build, market, manufacture, use, or sell the Findora Ledger and the Zei cryptography library;
- All documents and evidence in any form related to Eian, JVP, JVI, Project Revolution Fund, Onyx, and Real Time NY, LLC;
- All documents and evidence related to the luxury watch business that Chao and Ding are engaged in;
- All evidence related to the investors that Ariel Abittan introduced to Chao or Findora;
- All of your expenses relating in any way to Findora;
- All documents related to any transactions or purported or contemplated transactions between Temujin Labs Inc. and Eian, including but not limited to the Intellectual Property Sale Agreement with Eian;
- All documents related to Ariel Abittan's ownership interest in JVP, JVI, Eian, Temujin Labs Inc., Findora, and the watch business.

You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other

media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible meaning and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, optically or otherwise stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- E-Mail Server Stores (e.g., Lotus Domino .NSF or Microsoft Exchange .EDB)
- Word processed documents (e.g., Word or WordPerfect files and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, blog entries);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Telegram, Twitter, WeChat, iMessage and Other Social Media Accounts and Messaging Services;
- Computer Aided Design/Drawing Files; and
- Backup and Archival Files (e.g., Veritas, Zip, .GHO)

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem *not* reasonably accessible. You are obliged to *preserve* potentially relevant evidence from *both* sources of ESI, even if you do not anticipate *producing* such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to the rules of civil procedure, you must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible. For good cause shown, the court may order production of the ESI, even if it is not reasonably accessible. Accordingly, you must preserve ESI that you deem inaccessible so as not to preempt the court's authority.

PLEASE TAKE FURTHER NOTICE,

Preservation Requires Immediate Intervention.

You must act immediately to preserve potentially relevant ESI, including, without limitation, information with the earlier of a Created or Last Modified date on or after January 1, 2015 through the date of this demand and concerning:

1. The events and causes of action related to the facts in this matter as well as the events and causes of action contained in the draft complaint that we provided to you on December 20, 2020;

2. Any and all ESI you may use to support claims or defenses in this case;

3. Any non-privileged communications by and between any person concerning the subject matter of this case;

4. Any non-privileged communications by and between any or your agents, representatives and/or employees concerning the case; and

5. Any and all written documents, data and tangible things related to the claims in this case.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must intervene to prevent loss due to routine operations or malfeasance and employ proper techniques and protocols to preserve ESI. Booting a drive, examining its contents or running any application may irretrievably alter the evidence it contains and constitute unlawful spoliation of evidence.

Preservation requires action.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction.

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding backup media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;

- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server, packet or local instant messaging logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion.

You should anticipate that your officers, employees or others may seek to hide, destroy or alter ESI. You must act to prevent and guard against such actions. Especially where company machines were used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing, and in so doing, they may also delete or destroy potentially relevant ESI. This concern is not unique to you. It is simply conduct that occurs with such regularity that any custodian of ESI and their counsel must anticipate and guard against its occurrence.

Preservation of Backup Tapes.

You are directed to preserve complete backup tape sets (including differentials and incrementals) containing e-mail and ESI for all dates from January 1, 2015 to the present.

Act to Prevent Spoliation.

You should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide ESI on network or local hard drives and on other media or devices (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging, damaging or replacing media, encryption, compression, steganography or the like).

System Sequestration or Forensically Sound Imaging.

As an appropriate and cost-effective means of preservation, you should remove from service and securely sequester the systems, media and devices housing potentially relevant ESI.

In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices of those named above is expedient and cost effective. As we may anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

"Forensically sound ESI preservation" means duplication of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. The products of forensically sound duplication are called, inter alia, "bitstream images" or "clones" of the evidence media. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including deleted evidence within "unallocated clusters" and "slack space."

Be advised that a conventional copy, backup or "Ghosting" of a hard drive does not produce a forensically sound image because it only captures active, unlocked data files and fails to preserve forensically significant data existing in, e.g., unallocated clusters and slack space.

Further Preservation by Imaging.

With respect to the hard drives and storage devices, demand is made that you immediately obtain, authenticate and preserve forensically sound images of the hard drives in any computer system (including portable and home computers) used by Temujin Labs Inc. (Delaware), Temujin Labs Inc. (Cayman), Chao, Ding, Jianrong Wang, Selena Chen, Guanghua Liang, Eian, JVP, JVI, Project Revolution Fund, or Findora or any of its present or former employees during the period from January 1, 2015 to the present, as well as recording and preserving the system time and date of each such computer.

Once obtained, each such forensically sound image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

Preservation in Native Form.

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained (i.e., native form). Accordingly, you should preserve ESI in such native forms, and you should not employ methods to preserve ESI that remove or degrade the ability to search the ESI by electronic means or that make it difficult or burdensome to access or use the information.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata.

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files, but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Metadata may he overwritten or corrupted by careless handling or improper preservation, including by moving, copying or examining the contents of files.

Servers.

With respect to servers used to manage e-mail (e.g., Microsoft Exchange, Lotus Domino) and network storage (often called a "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server. If you are uncertain whether the preservation method you plan to employ is one that we will accept as sufficient, please immediately contact the undersigned.

Home Systems, Laptops, Online Accounts and Other ESI Venues.

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems or devices may contain potentially relevant data. To the extent that you have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CDR/DVD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.).

Similarly, if you used online or browser-based e-mail accounts or services (such as Gmail, AOL, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

Ancillary Preservation.

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters and the like.

You must preserve passwords, keys and other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate.

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys and Third Parties.

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian and contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

Preservation Protocols.

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol if you will furnish an inventory and description of the systems and media to be preserved. Alternatively, if you promptly disclose the preservation protocol you intend to employ, perhaps we can assist. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that is fair to both sides and acceptable to the court.

ALTO LITIGATION

Do Not Delay Preservation.

We are available to discuss reasonable preservation steps; however, *you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay*. Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Confirmation of Compliance.

Please confirm within the next thirty (30) days that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence. Thank you for your time and attention to this matter. If you have any questions, please do not hesitate to contact us.

Sincerely,

Joshua A. Korr, Esq.

Counsel for Ariel Abittan